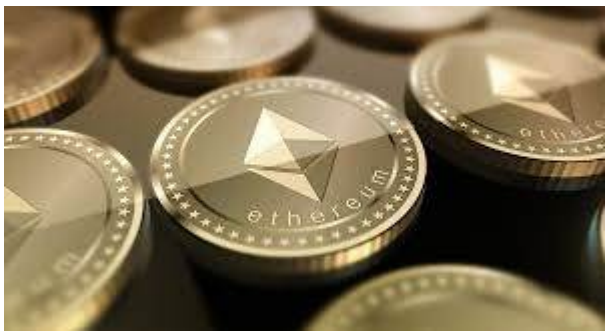
The Cyber-Security source
by Rene Millman
November 08, 2017

£214 million in Ethereum crypto-currency virtually gone after code deletion

Around one million Ethereum digital coins (approximately £214 million) have become inaccessible to users following the accidental deletion of code.



According to a security advisory by Parity Technology, the firm that provides digital wallets for Ethereum, it said a flaw was "accidentally" triggered which resulted in suspending more than £214 million worth of Ethereum.

Tuur Demeester, editor in chief at Adamant Research, claimed that of that figure, about £69 million belongs to Parity founder and former Ethereum core developer Gavin Woods' Initial Coin Offering (ICO) Polkadot.

"Following the fix for the original multi-sig issue that had been exploited on 19th of July (function visibility), a new version of the Parity Wallet library contract was deployed on 20th of July," the advisory stated.

The company said that the code contained another issue - it was possible to turn the Parity Wallet library contract into a regular multi-sig wallet and become an owner of it by calling the initWallet function. Parity said that the was triggered accidentally 6 Nov 2017 at 02.33PM and subsequently "a user suicided the library-turned-into-wallet, wiping out the library code which in turn rendered all multi-sig contracts unusable since their logic (any state-modifying function) was inside the library".

"This means that currently no funds can be moved out of the multi-sig wallets," the advisory warned.

Multi-sig (multiple signature) wallets require more than one person to agree money transfers as a safeguard against fraud.

Parity is still investigating how to correct the problem.

According to a blog post by Matt Suiche, founder of Comae|o, even though the vulnerable smart-contract was open source and deployed months ago, this bug managed to escape code review done by the Parity team.

“Since by design smart-contracts themselves can't be patched easily, this make dependencies on third party libraries very lethal if a mistake happens,” said Suiche.

“We have seen a lot of enthusiasm from a lot of people about blockchain-based smart contracts, and the general assumption from users is that they would be secure. But just like any other piece of software a smart-contract can be vulnerable.”

“All the recent security issues around smart contracts are challenging more and more the sustainability of storing money on a blockchain-based software layer,” he added.

Ilia Kolochenko, CEO of web security company High-Tech Bridge, told SC Media UK that crypto-currencies bring a great wealth of new opportunities to modern businesses.

“However, they unavoidably deliver a wide spectrum of contiguous risks. Crypto-currencies tend to create a semblance of reliability and security, but in fact they are widely exaggerated,” he said.

“Omitting complicated cryptographic and logic flaws in the code, attackers now have many new targets and an increased attack surface to steal valuable digital coins. Many stock exchanges and millions of wallets were compromised in the last few years via common vulnerabilities affecting systems that handle, store or process the digital currency. Worse, in many cases, it's technically impossible to get your money back even if the supreme court orders so,” he added.

“Law enforcement agencies struggle to trace and investigate skyrocketing data breaches affecting financial institutions and have no time or desire to take care of the unregulated market. Therefore, if you undertake a journey into crypto-currency realm, be well prepared to face the related risks.”

Dominic Williams, founder of DFINITY, told SC Media UK that the only method he was aware of to “unfreeze” tokens held by the vulnerable smart contract would be to create a new “hard fork” Ethereum client that deploys a fix.

“This would require every full node on the Ethereum network to upgrade by the date of the hard fork to stay in sync, including all miners, wallets, exchanges, etc.” he said.

“In contrast to the “hard fork” method of deploying network-wide changes, DFINITY will use its “Blockchain Nervous System” (BNS) to update protocol rules. This system will make it possible to deploy a change that would fix a bug such as the vulnerability affecting the Parity wallet without requiring every node on the network to manually update their software. Instead, the BNS will act autonomously, upgrading the protocol rules automatically once a threshold of support is reached for a given proposal.”

Derek Weeks, VP and DevOps Advocate, Sonatype adds that loss shows the urgent need for businesses and cryptocurrency firms to know what libraries and binaries they're using.

In an email to SC Media UK he commented, “With open source binaries forming the basis of 80 – 90 percent of applications, they play a vital role in driving innovation and powering the world as we know it. However, Parity's issues are a stark reminder that all binaries are not created equal.

“To address this, it is imperative that strict governance protocols are in place to determine which components are safe to use, and which ones are vulnerable. In Parity's case, the lack of such protocol

meant that a vulnerable component could be deployed in what should have been a highly governed environment, leading to the loss of hundreds of millions of dollars.

“Faults such as these should serve as a call to arms for legislators, and organisations that release known vulnerable code into production (especially when it can't be patched) should understand that they could be liable for gross negligence. This has already started to happen in the UK, with organisations that neglect to repair systems using vulnerable binaries incurring fines. As more and more legislators recognise the huge damage vulnerable components can cause, we expect to see an increasing number of nations following suit.

“Fortunately, the challenges of faulty components are easily solved by using a DevSecOps approach. This enables security and governance to be automated from the start and implemented everywhere within a DevOps pipeline. Instead of using manual reviews of code, which leaves businesses at risk of human error, DevOps practices can utilise machines to adjudicate all components. For Parity, this would have prevented the error and subsequent loss.”

Topics:

- Cryptocurrency
- Mistakes
- Ethereum

tokensale.liveedu.tv • 4 months ago

Its terrible what happend to people having parity tokens. I just don't get how you accidently delete something this important and not get sued...

Related Articles

[£23 million in Ethereum coins stolen from vulnerable multi-sig wallets]

BY Max Metzger Jul 20, 2017

Ethereum crypto-currency breach affects 16K

BY Robert Abel Dec 21, 2016

Bitcoin's booming valuation is helping attract more cybercriminals

BY Doug Olenick Sep 1, 2017

Hackers steal nearly £400K from Enigma virtual currency ICO investors

BY Bradley Barth Aug 22, 2017

Most read on SC

- Google gets sued for denying "right to be forgotten" request
- Hackers using blockchain to keep authorities at bay & to sustain operations
- Chrome 65 update ready, contains 45 security fixes
- Government calls for revamp in IoT security; will manufacturers listen?
- Hospitality industry is key infosec battleground

SC Media UK arms cyber-security professionals with the in-depth, unbiased business and technical information they need to tackle the countless security challenges they face and establish risk management and compliance postures that underpin overall business strategies.

USER CENTRE

About Us

Contact Us

Advertise

Partner's Corner

RESOURCES

Issue Archive

OTHER

Privacy Policy

Terms & Conditions

MORE SC SITES